What is claimed is:

1. A computer architecture for an intrusion detection system, comprising:

a control agent to interface with a management system and to monitor system activity;

at least one data gathering component which gathers kernel audit data and syslog data;

at least one correlator to interpret and analyzes the kernel audit data and the syslog data using at least one detection template.

2. The computer architecture of claim 1, wherein said intrusion detection system is host-based.

3. The computer architecture of claim 1, wherein said detection templates are configured into surveillance groups and into surveillance schedules.

4. The computer architecture of claim 1, wherein said management system includes a graphical user interface.

5. The computer architecture of claim 4, further comprising a communication agent which encrypts information sent from said intrusion detection system to said management station.

6. The computer architecture of claim 1, wherein there is low bandwidth connection between said control agent and each of said data gathering components and said at least one correlator and a high bandwidth connection between said control agent and each said data gathering component and said correlator.

7. The computer architecture of claim 1, wherein said correlator uses a meta-description language.

8. The computer architecture of claim 1, wherein said high bandwidth connection is used to send and receive memory-mapped files.

9. The computer architecture of claim 1, wherein said data gathering component includes a kernel audit record component and a syslog component.

10. The computer architecture of claim 9, wherein said data gathering component and said syslog component convert gathered data into an ASCII format.

11. The computer architecture of claim 1, further comprising a notification log and a response script connected to said control agent.

12. The computer architecture of claim 1, further comprising an installed bits file connected to said control agent.

13. The computer architecture of claim 1, wherein the computer architecture uses one of eglinux, solaris and windows 2000 operating system.

14. The computer architecture of claim 1, wherein the management system controls more than one control agent each residing on a different computer.

15. The computer architecture of claim 1, wherein said at least one template is selected from the group including:

reading kernel records;

reformatting each of the read kernel records into a different format;

parsing the records and comparing the parsed records against one or more templates.

16. The computer architecture of claim 1, wherein said control agent communicates with said management system across a secure communications link.

17. The computer architecture of claim 1, wherein if the correlator detects an intrusion an alert will be sent to the management system and a potential intrusion alert record will be logged to a notification file.

18. The computer architecture of claim 1, wherein said at lest one data gathering component includes a buffer.

19. A computer architecture for detecting intrusions, comprising:

reading means for reading kernel records;

reformatting means for reformatting each of the read kernel records into a different format;

parsing means for parsing the records and comparing the parsed records against one or more templates.

20. The computer architecture of claim 19, wherein the at least one template is selected from the group including:

a modification of files/directories template;

a change to log files template;

a SetUID files template;

a creation of world-writables template;

a repeated failed logins template;

a repeated failed SU commands template;

a race conditions attack template;

a buffer overflow attacks template;

a modification of another user's file template;

a monitor for the start of interactive sessions template; and

a monitor logins/logouts template.

21. A computer system, comprising:

a processor; and

a memory coupled to said processor, the memory having stored therein sequences of instructions, which, when executed by said processor, causes said processor to perform the steps of:

reading kernel records;

reformatting each of the read kernel records into a different format;

parsing the records and comparing the parsed records against one or more templates.

22. The computer system of claim 22, wherein the at lest one template is selected from the group including:

a modification of files/directories template;

a change to log files template;

a SetUID files template;

a creation of world-writables template;

a repeated failed logins template;

a repeated failed SU commands template;

a race conditions attack template;

a buffer overflow attacks template;

a modification of another user's file template;

a monitor for the start of interactive sessions template; and

a monitor logins/logouts template.